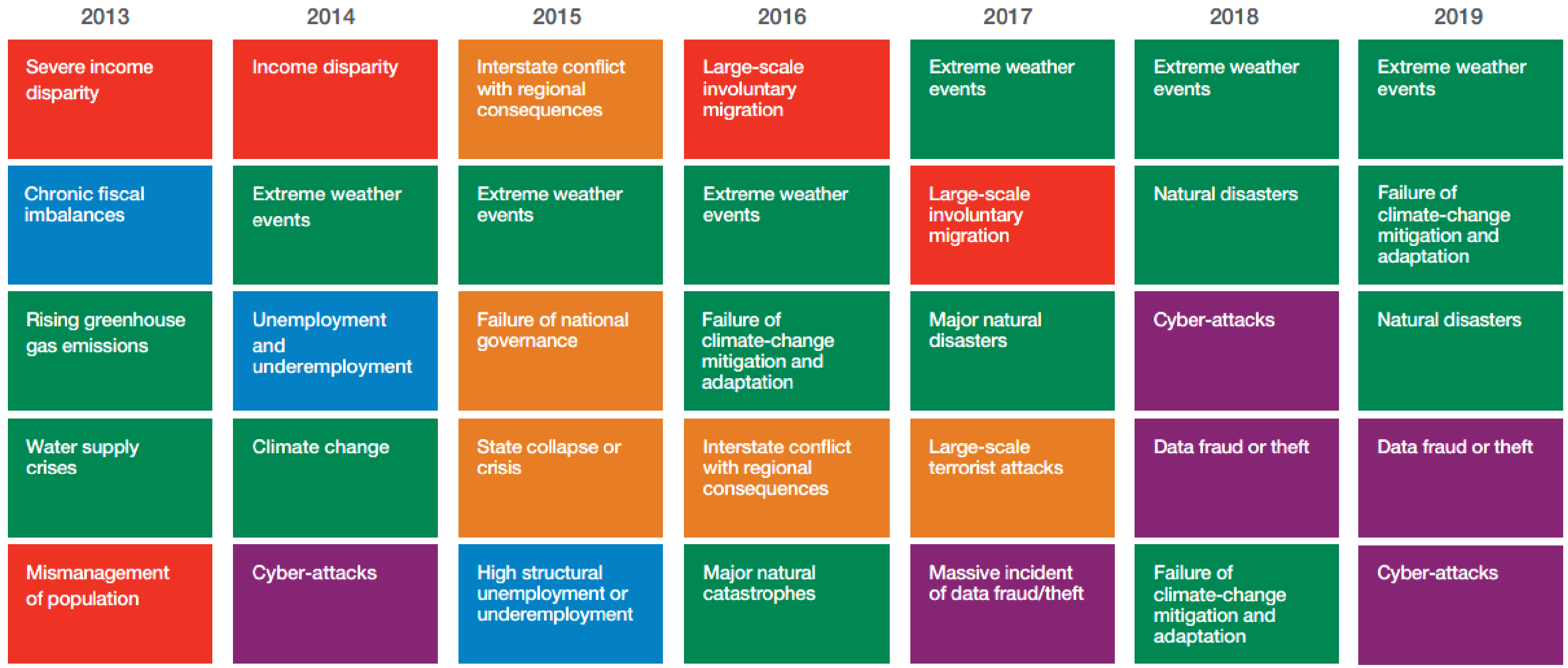
# Cybersecurity: Governance and Best Practices in a Shifting Threat Landscape

Presenter: Aravind Swaminathan

# Global Cybersecurity Risk

*“Last year also provided further evidence that cyber-attacks pose risks to critical infrastructure, prompting countries to strengthen their screening of cross-border partnerships on national security grounds.”*

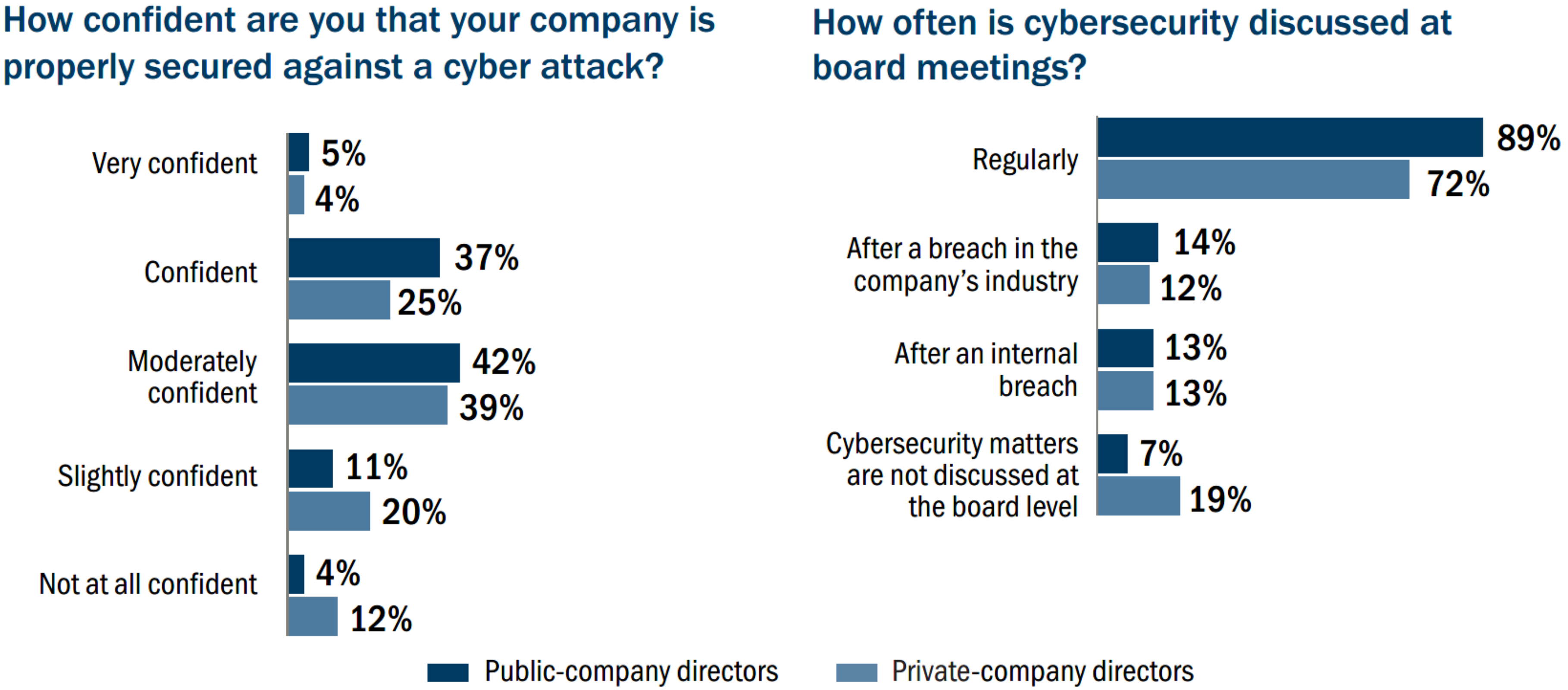


| 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|
| Severe income disparity | Income disparity | Interstate conflict with regional consequences | Large-scale involuntary migration | Extreme weather events | Extreme weather events | Extreme weather events |
| Chronic fiscal imbalances | Extreme weather events | Extreme weather events | Extreme weather events | Large-scale involuntary migration | Natural disasters | Failure of climate-change mitigation and adaptation |
| Rising greenhouse gas emissions | Unemployment and underemployment | Failure of national governance | Failure of climate-change mitigation and adaptation | Major natural disasters | Cyber-attacks | Natural disasters |
| Water supply crises | Climate change | State collapse or crisis | Interstate conflict with regional consequences | Large-scale terrorist attacks | Data fraud or theft | Data fraud or theft |
| Mismanagement of population | Cyber-attacks | High structural unemployment or underemployment | Major natural catastrophes | Massive incident of data fraud/theft | Failure of climate-change mitigation and adaptation | Cyber-attacks |

***Source: World Economic Forum Global Risks 2019***

# Board Cyber Oversight Is Increasing/Improving

FIGURE 1

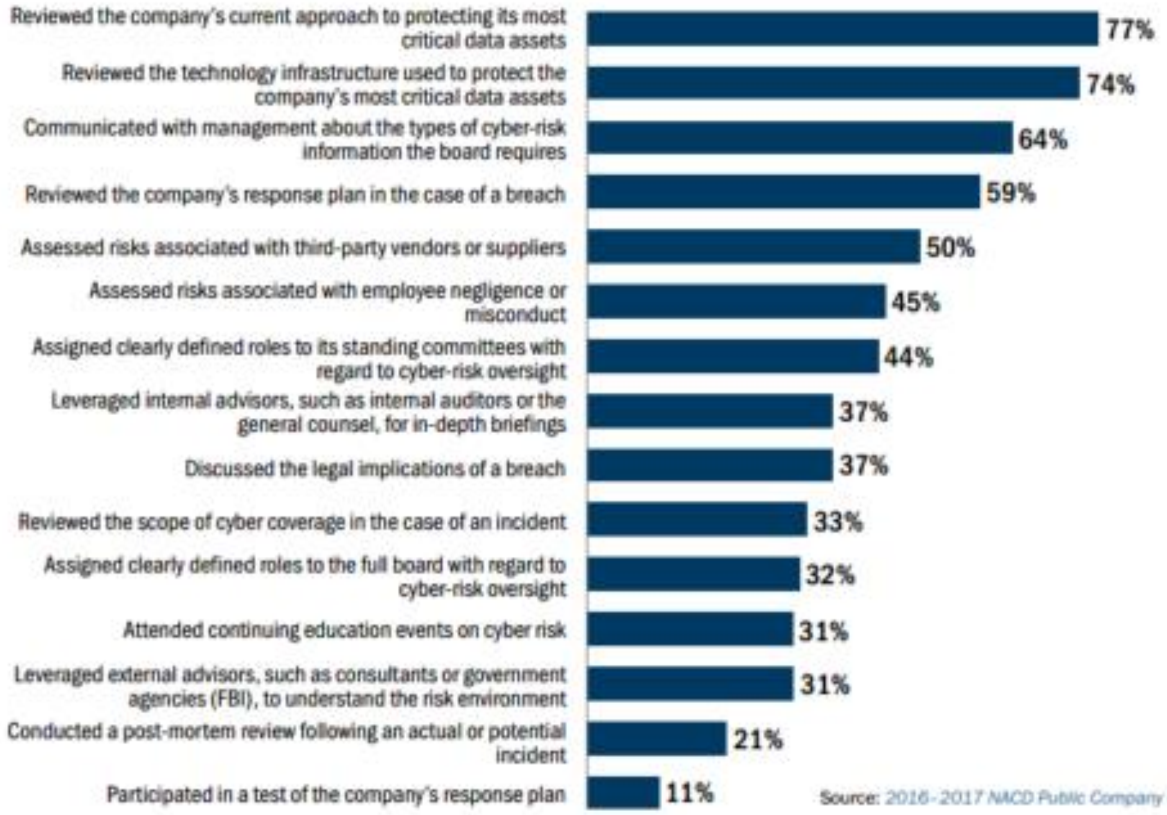


Source: This data is compiled from the NACD 2016–2017 public- and private-company governance surveys.

# Fiduciary Duties

- Duty of care
  - Duty to monitor
  - Delegation
  - Maintenance of retirement system confidential information
  - Prudence
    - Asking questions and understanding the rationale for actions before taking them
    - Analyzing advice and recommendations received from experts (not a rubber stamp)
- Duty of loyalty

# What are Board members doing to fulfill their fiduciary duties?



Source: *2016-2017 NACD Public Company Governance Survey*

- Not all Boards are doing the same things.
- There is no "answer" or "recipe" that is easy to follow.
- Every Board should think through the issues, and develop an approach that "makes sense" for it and the organization.

# Key Questions for Boards to Ask of Management

- What are our **top cybersecurity risks**, and **what are we doing** to address those risks? Should we be worried about ransomware, nation state actors, insiders, phishing attacks, business email compromise, etc.? What is our risk tolerance?
- Do we understand our most **critical systems and data assets**? Do we have an **inventory of data and assets** that might be subject to compromise (e.g., data map or network map)?
- Are both **outside and inside threats** considered when planning cybersecurity program activities? Do we have comprehensive internal cybersecurity **policies and procedures**?
- Who in management has **primary cybersecurity risk oversight responsibility** (e.g., CISO)? If so, who does she report to? Are her and her team **adequately resourced** – both staff expertise and budget?
- Do we use a **security framework**, such as National Institute for Standards and Technology (NIST) Cybersecurity Framework? Do we have a **security roadmap** for identifying progress and enhancements?
- Do we conduct **periodic technical and risk assessments**? Do we base remediation and security improvements on identified risks?

# Key Questions for Boards to Ask of Management

- Does every **employee** receive some basic cybersecurity awareness training?  Do they understand their roles and responsibility for cybersecurity?
- Do we use **encryption** to protect data in transit and at rest?  Do we have an established process for patching and managing **system vulnerabilities**?  Do we restrict **access privileges** for staff?
- What **risks do vendors present**?  Is security a criteria in selecting vendors?  Do we require minimum level of security from vendors, and test them regularly?
- Do we participate in **threat intelligence sharing forums** to develop understanding of threat landscape (e.g., FS-ISAC)?  Are we proactively engaged with **law enforcement**?
- In the event of a cyberattack, has management developed a robust **incident response plan**?  Do we have outside resources that may be necessary if there’s an attack?  Do we practice regularly?
- Do we have cyber liability or other insurance to cover costs of forensic analysis, legal services, public relations, credit monitoring, litigation defense, etc.?